UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/898,310	07/03/2001	Teng Pin Poo	1601457-0008	2223

7470 7590 11/12/2008

WHITE & CASE LLP
PATENT DEPARTMENT
1155 AVENUE OF THE AMERICAS
NEW YORK, NY 10036

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
11/12/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/898,310
Filing Date: July 03, 2001
Appellant(s): POO ET AL.

Warren S. Heit
Reg. No. 36,828
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 8/29/08 appealing from the Office action mailed 7/10/07.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,671,808	Abbott et al.	12-2003
7036738	Vanzini et al.	05-2003
20020145507	Foster	10-2002
5815252	Price-Francis	09-1998
20010045458	Polansky	11-2001
6990587	Willins et al.	10-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-2, 4-5, 7-8, 11-12, 14-15, 17-18, 20, 23, 25 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Abbott et al. (hereinafter Abbott) United States Letters Patent No. 6,671,808 in view of Vanzini et al. (hereinafter Vanzini) Unites States Patent Number 7,036,738.

As per claims 1, 11 and 17:

Abbott teach a unitary portable biometric-based access control device which can be directly plugged into a universal serial bus (USB) socket communicatively coupled to a restricted resource, the device comprising:

housing; (figure 1, item 200)

a microprocessor housed within the housing; (col. 3, lines 29-31)

a memory coupled to the microprocessor and capable of storing user data; (col. 3, lines 29-41)

a USB plug integrated into the housing without an intervening cable and capable of coupling the unitary portable access control device directly to the USB socket; (figure 1, item 130; col. 3, lines 27-29) and

a biometrics-based authentication module coupled to and controlled by the microprocessor, at least a portion of the biometrics-based authentication module being housed within the housing, wherein said biometrics-based authentication module is configured to grant access to the restricted resource provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the restricted resource is denied to the user otherwise; (col. 3, lines 47-52; col. 7, line 60- col. 8, line 6) and further wherein

said biometrics-based authentication module is configured to grant access to the user data (col. 3, lines 45-52; col. 6, line 66-col. 7, line 16; virtually all of user's sensitive information; user's calendar, user's private data) stored in the memory provided that the biometrics-based authentication module authenticates the user's identity and wherein access to the user data stored in the memory is denied to the user otherwise. (col. 3, lines 47-52; col. 7, line 60- col. 8, line 6)

Abbott does not explicitly disclose a non-volatile memory having a minimum of 8MB of capacity. Vanzini in analogous art, however, teaches a non-volatile memory having a minimum of 8MB of capacity. (col. 4, lines 24-49; col. 5, line 26-col. 6, line 9) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Abbott with Vanzini in order to provide a portable data carrier that stores and securely transports a user's

profile and data files with a substantial amount of user data. (Abstract, col. 4, line 47; Vanzini)

As per claims 2, 12 and 18:

The combination of Abbott and Vanzini teaches all the subject matter as discussed above. In addition, Abbott further discloses the biometrics-based authentication module is a fingerprint authentication module. (col. 3, lines 46-48)

As per claims 4 and 14:

The combination of Abbott and Vanzini teaches all the subject matter as discussed above. In addition, Abbott further discloses the biometrics-based authentication module comprises a biometrics sensor fitted on one surface of the housing. (figure 2A, item 250)

As per claims 5 and 15:

The combination of Abbott and Vanzini teaches all the subject matter as discussed above. In addition, Abbott further discloses a non-volatile memory capable of storing biometrics information usable for authentication. (col. 3, lines 47-52; col. 7, line 60- col. 8, line 6)

As per claim 7:

The combination of Abbott and Vanzini teaches all the subject matter as discussed above. In addition, Abbott further discloses the restricted resource comprises a host computer. (figure 1, item 102)

As per claim 8:

The combination of Abbott and Vanzini teaches all the subject matter as discussed above. In addition, Abbott further discloses the restricted resource comprises a communication network. (col. 3, lines 41-43)

As per claim 20:

The combination of Abbott and Vanzini teaches all the subject matter as discussed above. In addition, Abbott further discloses the step of denying the user access to the restricted resource provided that a match is not identified in said step (d). (col. 3, lines 47-52; col. 7, line 60- col. 8, line 6)

As per claims 23, 25 and 27:

The combination of Abbott and Vanzini teaches all the subject matter as discussed above. In addition, Vanzini further wherein the non-volatile memory has capacity sufficient to serve as a mass-storage device. (col. 4, lines 24-49; col. 5, line 26- col. 6, line 9)

3. Claims 3 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Abbott et al. (hereinafter Abbott) United States Letters Patent No. 6,671,808 in view of Vanzini et al. (hereinafter Vanzini) Unites States Patent Number 7,036,738 and further in view of Foster United States Publication number 2002/0145507.

4. As per claims 3 and 13:

5. The combination of Abbott and Vanzini teaches all the subject matter as discussed above. Both references do not explicitly disclose a device wherein the

biometrics-based authentication module is an iris scan authentication module. Foster in analogous art, however, discloses a device wherein the biometrics-based authentication module is an iris scan authentication module. (page 1, paragraph 12; page 2, paragraph 20) Therefore, a person having ordinary skill in the art at the time the invention was made would have been motivated to modify the method disclosed by Abbott and Vanzini with Foster in order to provide a versatile biometric authentication device that is not restricted only to fingerprint.

6. Claims 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Abbott et al. (hereinafter Abbott) United States Letters Patent No. 6,671,808 in view of Vanzini et al. (hereinafter Vanzini) Unites States Patent Number 7,036,738 and in view of Polansky United States Publication Number 2001/0045458.

7. As per claim 9:

8. The combination of Abbott and Vanzini teaches all the subject matter as discussed above. Both references do not explicitly disclose the restricted resource is a real estate premises that imposes access restrictions. Polansky in analogous art, however, teaches the restricted resource is a real estate premises that imposes access restrictions. (page 2, paragraph 25) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Abbott and Vanzini with Polansky in order to provide an open, stand-alone system that protects the real estate premises by enforcing proper biometric authentication.

As per claim 10:

The combination of Abbott and Vanzini teaches all the subject matter as discussed above. Both references do not explicitly the restricted resource is an operable machinery, the safe operation of which requires training. Polansky in analogous art, however, teaches the restricted resource is an operable machinery, the safe operation of which requires training. (page 2, paragraph 25) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Abbott and Vanzini with Polansky in order to provide an open, stand-alone system which protects the machinery by enforcing proper biometric authentication.

9. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Abbott et al. (hereinafter Abbott) United States Letters Patent No. 6,671,808 in view of Vanzini et al. (hereinafter Vanzini) Unites States Patent Number 7,036,738 and further in view of Willins et al. (hereinafter Willins) U.S. Patent 6,990,587.

As per claim 19:

The combination of Abbott and Vanzini teaches all the subject matter as discussed above. Both references do not explicitly disclose the registered biometrics marker is stored in an encrypted format. Willins in analogous art, however, discloses a biometrics marker is stored in an encrypted format. (col. 5, lines 33-67) Therefore, a person having ordinary skill in the art at the time the invention was made would have been motivated to modify the method disclosed by Abbott and Vanzini to with Willins in order to provide increased security by protecting the biometric data being access by unauthorized person.

10. Claims 22, 24 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Abbott et al. (hereinafter Abbott) United States Letters Patent No. 6,671,808 in view of Vanzini et al. (hereinafter Vanzini) Unites States Patent Number 7,036,738 and further in view of Terasaki U.S. Publication Number 2001/0004326 (hereinafter Terasaki).

11. As per claims 22, 24 and 26:

12. The combination of Abbott and Vanzini teaches all the subject matter as discussed above. In addition, Vanzini further discloses a data memory can be implemented as flash memory, on the order of currently up to 128 MB. Both references do not explicitly disclose wherein the non-volatile memory has a maximum of 512 MB of capacity. Terasaki in analogous art, however, discloses wherein the non-volatile memory has a maximum of 512 MB of capacity. (page 11, paragraph 172) Therefore, a person having ordinary skill in the art at the time the invention was made would have been motivated to modify the method disclosed by Abbott and Vanzini to with Terasaki in order to reduce the time for formatting a flash memory thereby increasing throughput and decreasing cost. (Page 11, paragraph 172; Terasaki)

Allowable Subject Matter

13. Claims 6, 16 and 21 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter: None of the prior art either taken singularly or in combination teach "a microprocessor is configured to provide a bypass mechanism for authentication upon a determination of authentication failure by the biometrics-based authentication module" including all the limitations of the base claim and any intervening claims.

(10) Response to Argument

Appellant's arguments filed 8/29/08 with respect to the rejection of claims 6, 16 and 21 have been fully considered and are persuasive. The rejection of claims 6, 16 and 21 has been withdrawn. The rest of Appellant's arguments have been fully considered but they are not persuasive. In response to the Appellant's arguments the following comments are made:

With respect to claims 1, 11 and 17:

The Appellant argued that *"the biometric sensor of Abbott only has function: controlling access to passwords stored in the personal key."* The Examiner respectfully disagrees. Abbott discloses that a USB-compliant personal key that includes a processor, a memory with a biometric sensor for authenticating the identity of the user. The biometric sensor is sized and disposed to collect data from the user's thumbprint when the user grips the personal key to insert it into the host computer. Alternatively to increase security, the housing may be designed to mask the presence of the biometric sensor entirely. ***The biometric sensor can be advantageously placed in a position where it can be expected to collect known data of a predictable type, at a known***

time for example, obtaining a thumbprint when the personal key is plugged into the host computer I/O port. The personal key accepts data from the biometric sensor to verify the identity of the person holding the key with no passwords to remember or compromise, or any other input. (col. 6, lines 65-67; col. 7, lines 17-67) Therefore, Abbott not only teaches a biometric sensor to control access to the data stored in the personal key but also control access to a host computer (i.e. restricted resource) by verifying the identity of the person which is adequate to meet the claimed limitation "*a biometrics-based authentication module to grant access to the restricted resource*" as recited in the independent claims.

The Appellant argued that "*Abbott's disclosure, the passwords stored on the personal key enable access to a restricted resource (e.g., software on a host computer). The biometrics module of Abbott unlocks the set of passwords stored on the personal key, and one of the stored passwords unlocks a restricted resource. If a user successfully gains access the passwords on the personal key using the biometrics module, the user cannot access a restricted resource unless the personal key contains the correct password for that resource. With Abbott's personal key, a successful biometrics-based authentication only allows access to the passwords stored on the personal key.*" Examiner would like to point out that contrary to Appellant's argument; Abbott specifically discloses that ***when the personal key is plugged into the host computer, the personal key accepts data from the biometric sensor to verify the identity of the person holding the key with no passwords to remember or compromise, or any other input.*** (col. 7, lines 64-67)

Appellant argued that *"by teaching storage of multiple passwords in a personal key where the passwords are required for access to restricted resources, Abbott teaches away from using a biometrics-based authentication module to control access to a restricted resource."* Abbott discloses a personal key comprising biometric sensor for authenticating the identity of the user, by obtaining a thumbprint when the personal key is plugged into the host computer to identify the identity of the person holding the key and since the personal key represents a single, secure repository for a great deal of the user's private data, it is important the personal key as secure as possible by measuring the characteristics of the person holding the key to confirm that the person holding the key is the actual owner of the key. (col. 7, lines 64-67)

Appellant argued that "*Abbott's biometrics-based authentication has only one function: controlling access to passwords stored on personal key."* First, the personal key disclosed by Abbott ***stores not only passwords but also digital certificates, cookies, Java-implemented software programs and instructions such as the user's calendar or other user data*** (col. 3, lines 32-41; col. 6, lines 65-67). Secondly, Abbott discloses that when the personal key is plugged into the host computer, the personal key accepts data from the biometric sensor to verify identify of the person holding the key with no passwords to remember or compromise or any other input (*i.e. using biometrics-based authentication to allow access to a restricted resource*).

Appellant argued that "*Abbott also does not disclose the limitation, controlling access to user data stored in a non-volatile memory with a minimum of 8 MB of capacity.*" Appellant is arguing the references individually, the combination of Abbott

and Vanzini is used for teaching the limitation. Abbott discloses a personal key with a memory storing virtually all of the user's sensitive information as well as a repository for a great deal of the data the user will need to use and interact with a variety of computer platforms and to store programs and instruction such as user's calendar. (col. 6, lines 65-67). Although Abbott discloses a memory to store user data, Abbott does not explicitly disclose the type and size of memory in the personal key. However, Vanzini discloses a portable profile carrier for transporting user profile and user files in a secured medium. ***The data memory can be implemented as flash memory, on the order of currently up to 128 MB, to hold substantial amount of user data.*** Authorization to access user profile is achieved by authenticating the user via a passcode challenge. (col. 4, lines 45-47; col. 6, lines 4-6) Therefore, Vanzini teaches ***a flash memory up to 128 MB to hold user data*** **and user profile** and performing user authentication via a passcode challenge before allowing access which meets the claimed limitation "*a non-volatile memory coupled to the microprocessor and capable of storing user data and having a minimum of 8 MB of capacity*" as cited in the instant application.

Appellant argued that "Vanzini's *tow-part system teaches away from the device of claim 1, … Vanzini requires the user to enter a password to authenticate to the smartcard."* Examiner would like to point out that Vanzini is used for teaching only the non-volatile memory capable of storing user data and having a minimum of 8 MB of capacity. Examiner agrees with the Appellant that Vanzini teaches authenticating a user using a passcode before allowing access to a user data stored in the memory of the

smart card, however, Abbott is used for teaching a biometric-based authentication not Vanzini.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992) In this case, Abbott discloses a personal key comprising biometric sensor for authenticating the identity of the user, by obtaining a thumbprint when the personal key is plugged into the host computer to identify the identity of the person holding the key and since the personal key represents a single, secure repository for a great deal of the user's private data, it is important the personal key as secure as possible by measuring the characteristics of the person holding the key to confirm that the person holding the key is the actual owner of the key. (col. 3, lines 32-62; col. 7, lines 17-67) Vanzini discloses a portable profile carrier for transporting user profile and user files in a secured medium. The data memory can be

implemented as flash memory, on the order of currently upto 128 MB, to hold substantial amount of user data and authenticating the user via a passcode challenge before allowing access to the user data. (col. 4, lines 45-47; col. 6, lines 4-6) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Abbott with Vanzini ***increase the capacity of the memory storage for holding a substantial amount of user data.*** (col. 4, line 48; Vanzini)

With respect to claims 3 and 13:

Appellant argued that "*there is no teaching or suggestion in Foster that the biometric device may be a part of a device that can be directly plugged into a USB socket communicatively coupled to a restricted resource*." Examiner would like to respectfully point out that, Appellant is arguing the references individually, the combination of Abbott, Vanzini and Foster is used for teaching "a biometric-authentication module is an iris scan authentication module". Although Abbott discloses ***a biometrics sensor that measures the characteristics of a person*** holding the key, Abbott does not explicitly disclose an iris scan authentication module as recited in claims 3 and 13. However, Foster discloses ***a device with which a biometric security system is integrated to measure user's characteristics, such as fingerprint or iris pattern*** (page 1, paragraph 12; page 2, paragraph 20) which is adequate to meet the claimed limitation.

In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections

are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

With respect to claims 6, 16 and 21:

The claims have been objected for being dependent on a rejected claim. (*see section 9, above*)

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Shewaye Gelagay/

Examiner, Art Unit 2437

Conferees:

Emmanuel Moise
/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437

Matthew Smithers
/Matthew Smithers/
Primary Examiner, Art Unit 2437